UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/996,948	11/27/2001	Chinna Narasimha Reddy Pellacuru	50325-0607	2395

29989 7590 10/05/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/996,948	PELLACURU, CHINNA NARASIMHA REDDY	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 27 November 2001.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 27 November 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 11/27/2001.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-8,10,12-14,16-22,24-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Trostle et al (herein after referred as Trostle). (US Pub No 2005/0097317)

4. As per claim 1: Trostle discloses a method for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving, from a first node, a first request to store an encryption key, wherein

the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;[0050][0053]

in response to the first request

storing the encryption key; [0049]

creating and storing an association between the encryption key and the identifier;[0028][0049][0050]

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; [0028][0048]

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key;[0028 and 0049]; and

sending the encryption key to the at least one second node for use in

decrypting the encrypted data. [0050]

5. As per claim 2: Trostle discloses a method wherein:

a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key;[0049 and 0050]

the first node is a router that acts as a multicast originator[0047]; and

the plurality of second nodes is a plurality of routers that act as multicast receivers.[0047]

6. As per claim 3: Trostle discloses a method wherein the trusted third party is selected from the group consisting of a certificate authority, a key distribution center, a key exchange authority, and a key exchange center [0050 and 0055].

7. As per claim 4: Trostle discloses a method wherein the step of receiving the first request includes the step of: receiving a third request to register the encryption key and the identifier. [0028 and 0062]

8. As per claim 5: Trostle discloses a method wherein the steps of creating and storing the association include the step of:

registering a certificate that includes the encryption key and the identifier.[0028, 0060, 0062]

9. As per claim 7: Trostle discloses a method further comprising the computer-implemented steps of:

in response to the first request, associating an expiration time with the encryption key;

in response to the second request, determining based on the expiration time whether the encryption key has expired[0079 and 0081]; and

when the encryption key has not expired, performing the steps of retrieving and sending the encryption key.[0079 and 0081]

10. As per claim 8: Trostle discloses a method further comprising the computer-implemented steps of:

registering the first node; and registering the first node[0060 and 0074]; and

registering one or more nodes of the plurality of second nodes.[0060 and 0074]

11. As per claim 10: Trostle discloses a method wherein the encryption key is selected from the group consisting of a private key, shared key, a pseudo-random string of bits, and a pseudo-random string of characters. [0066,0067]

12. As per claim 12: Trostle discloses a method wherein the first request includes a list of authorized second nodes, and further comprising the computer-implemented steps of:

in response to the first request, storing the list of authorized second nodes; [0060]

in response to the second request, determing whether the at least one second node is included in the list of authorized second nodes[0060 and 0062];and

when the at least one second node is included in the list of authorized second nodes,[0060 and 0062]

performing the steps of retrieving and sending the encryption key.[0060, 0062]

13. As per claim 13: Trostle discloses a method further comprising the computer-implemented steps of:

storing a list of nodes;[0049]

in response to the first request, determining whether the first node is included in the list of nodes;[0062]

when the first node is included in the list of nodes, performing the steps of storing the encryption key and creating and storing the association between the encryption key and the identifier.[0028 ,0029, 0049]

14. As per claim 14: Trostle discloses a method further comprising the computer-implemented steps of :

in response to the first request, associating one or more criteria with the encryption key;[0028]

in response to the second request, determining based on the one or more criteria whether the encryption key is valid[0028]; and

when the encryption key is valid, performing the steps of retrieving and sending the encryption key.[0028, 0049]

15. As per claim 15: Trostle discloses a method wherein the encryption key is an old encryption key, the identifier is an old identifier, and the association is an old association, and further comprising the steps of:

in response to the first request, associating one or more criteria with the encryption

key;[0028]

in response to the second request, determining based on the one or more criteria whether the encryption key is valid; and[0028]

when the encryption key is not valid,[0028]

receiving a third request to store a new encryption key, wherein the third request includes a new identifier, and wherein the new encryption key is used to encrypt additional data that is multicast with the new identifier to the plurality of second nodes;[0079 and 0081]

in response to the third request,

storing the new encryption key;[0049]

creating and storing a new association between the new encryption key and the new identifier;[0028, 0049]

receiving, from at least one additional second node of the plurality of second nodes, a fourth request to obtain the new encryption key, wherein the fourth request includes the new identifier;[0029 and 0075]

in response to the fourth request, [0079 , 0087]

16. As per claim 16: Trostle discloses a method wherein the data that the first node encrypts and multicasts is received from a source node. [0106, 0048]

17. As per claim 17:Trostle discloses a method

wherein:

the identifier is a session identifier;[0053]

the encrypted data is multicast with an originator identifier that is base identity of the first node;[0028,0050]

the second request includes an unverified originator identifier[0076]; and

further comprising the computer-implemented steps of:

in response to the first request, associating the originator identifier with session identifier[0050,0053]; and

in response to the second request, determining whether the unverified originator identifier is valid based on the originator identifier a informing the at least one second node whether the unverified originator is valid.[0050,0053,0070]

18. As per claim 18:Trostle discloses a method wherein:

a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key;[0049-0050]

the first request is encrypted based on a public key that is associated with the trusted third party; and[0028-0029,0050]

the first request is signed with a private key[0050]

19. As per claim 19: Trostle discloses a method wherein a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and

storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key, and further comprising the computer-implemented steps of: prior to sending the encryption key,[0049-0054]

encrypting the encryption key based on a public key that is associated with the at least one second node[0029] ;and

signing the encrypted encryption key with a private key that is associated with the trusted third party.[0049-0050] and [0055]

20. As per claim 20: Trostle discloses a method wherein the identifier is selected from the group consisting of a hostname, an Internet protocol address, a media access control address, an internet security protocol security parameter index, a first string of pseudo-random bits, a second string of pseudo-random characters, a third string of arbitrary bits, and a fourth string of arbitrary characters.[0029,0066-0067]

21. As per claims 21:Trostle discloses a method for encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of :

sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; [0028][0049][0050]

encrypting data based on the encryption key; and[0029]

multicasting the encrypted data with the identifier to one or more receiving nodes,[0028][0050]

wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.[0028,0029,0050]

22. As per claim 22: Trostle disclose a method for decrypting encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of :

receiving from an originating node a multicast that includes encrypted data and an identifier[0028,0029];

identifying the identifier from the multicast; [0079]

sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data; in response to the request to the authoritative node, [0028,0029,0062]

receiving the encryption key; and decrypting the encrypted data based on the encryption key. [0029]

23. As per claim 24: Trostle discloses a computer-readable medium carrying one or more sequences of instructions for facilitating secure communications among multicast nodes in a telecommunications network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;[0050][0053]

in response to the first request

storing the encryption key; [0049]

creating and storing an association between the encryption key and the identifier;[0028][0049][0050]

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; [0028][0048]

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key;[0028 and 0049] and

sending the encryption key to the at least one second node for use in decrypting the encrypted data. [0050]

24. As per claims 25:Trostle discloses a computer-readable medium carrying one or more sequences of instructions for encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of :

sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; [0028][0049][0050]

encrypting data based on the encryption key; and[0029]

multicasting the encrypted data with the identifier to one or more receiving nodes,[0028][0050]

wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.[0028,0029,0050]

As per claims 25:Trostle discloses a computer-readable medium carrying one or more sequences of instructions for encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of :

sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; [0028][0049][0050]

encrypting data based on the encryption key; and[0029]

multicasting the encrypted data with the identifier to one or more receiving nodes,[0028][0050]

wherein the one or more receiving nodes use the identifier to retrieve the

encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.[0028,0029,0050]

25. As per claim 26: Trostle discloses an apparatus for facilitating secure communications among multicast nodes in a telecommunications network, comprising:
means for receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;[0050][0053]

in response to the first request

means storing the encryption key, in response to the first request [0049]
means creating and storing an association between the encryption key and the identifier;[0028][0049][0050]
means for receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; [0028][0048]
means for retrieving the encryption key, in response to the second request

based on the identifier included in the second request and the association between the encryption key and the identifier[0028 and 0049] and
means for sending the encryption key to the at least one second node for use in decrypting the encrypted data. [0050]

26. As per claim 27:Trostle discloses an apparatus for encrypting communications among multicast nodes in a telecommunications network, comprising:
means sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; [0028][0049][0050]
means for encrypting data based on the encryption key; and[0029]
means for multicasting the encrypted data with the identifier to one or more receiving nodes,[0028][0050]
wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.[0028,0029,0050]

28. As per claim 28:an apparatus for facilitating secure communications among multicast nodes in a telecommunications network, comprising:
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;[0050][0053]

in response to the first request

storing the encryption key; [0049]

creating and storing an association between the encryption key and the identifier;[0028][0049][0050]

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; [0028][0048]

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key;[0028 and 0049] and

sending the encryption key to the at least one second node for use in decrypting the encrypted data. [0050]

29. As per claim 29: Trostle discloses an apparatus for encrypting communications among multicast nodes in a telecommunications network, comprising:

A processor;

One or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

sending an encryption key and an identifier that is associated with the

encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; [0028][0049][0050]

encrypting data based on the encryption key; and[0029]

means for multicasting the encrypted data with the identifier to one or more receiving nodes,[0028][0050]

wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.[0028,0029,0050]

Claim Rejections - 35 USC § 103

30. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle US Pub No 2005/0097317 in view of Yung-Kao Hsu US Patent No 5982898.

32. As per claim 6: Trostle discloses a method as recited in Claim 5, further comprising the computer-implemented steps of: in response to the first request, associating an expiration time with the encryption key; in response to the second request, determining based on the expiration time whether the encryption key has expired [0079 and 0081]. Trostle does not explicitly teach further when the encryption key has expired, revoking the certificate. However Yung-Kao Hsu teaches when the encryption key has expired, revoking the certificate. (column 3 lines 19-37). Therefore it would be obvious to one having ordinary skill in the art at the time the invention was made to employ the method of Yung-Kao Hsu with the system of Trostle in order to achieve secure communication among multicast group communication.

33. Claims 9,11 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle US Patent No 2005/0097317 A1 in view of Turtiainen et al (herein after referred to Turtianinen) US Pub No 2002/0059516 A1.

34. As per claim 9: Trostle discloses a method for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to

encrypt data that is multicast with the identifier to a plurality of second nodes;[0053][0050]

in response to the first request[0049]

storing the encryption key; [0049]

creating and storing an association between the encryption key and the identifier;[0028][0049][0050]

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; [0048][0028]

in response to the second request,[

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key;[0028 and 0049] and

sending the encryption key to the at least one second node for use in decrypting the encrypted data[0050].Trostle does not explicitly discloses further comprising the computer-implemented stepsof : generating the encryption key based on an Internet key exchange protocol with the first node. However, Turtiainen teaches a method further comprising the computer-implemented steps of: generating the encryption key based on an Internet key exchange protocol with the first node [0012-0014][0033]. Therefore it would be obvious to one having ordinary skill in the art at the time the invention was made to employ the method of Turtianinen with the system of Trostle in order to achieve secure communication among multicast group communication.

35. As per claim 11:Trostle discloses a method as recited in claim 1.Trostle does not explicitly disclose a method wherein: the first node uses the encryption key and Internet protocol security (IPsec) to encrypt the data that is multicast; and the at least one second node decrypts the encrypted data based on the encryption key and IPsec. However, Turtianinen teaches a method wherein: the first node uses the encryption key and Internet protocol security (IPsec) to encrypt the data that is multicast; and the at least one second node decrypts the encrypted data based on the encryption key and IPsec [0012-0014] [0033]. Therefore it would be obvious to one having ordinary skill in the art at the time the invention was made to employ the method of Turtianinen with the system of Trostle in order to achieve secure communication among multicast group communication.

36. As per claim 23:The combined teachings of Trostle and Turtiainen are relied upon disclosing a method wherein: a certificate authority to facilitate communications based on Internet protocol security (IPsec) among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: Trostle teaches:

receiving, at the certificate authority from a first router that acts as a multicast Originator, a first request to register an encryption key, wherein the first request includes a multicast session identifier and a list of authorized multicast receivers, and wherein the first router uses the encryption key to encrypt data

and multicasts the encrypted data with the multicast session

identifier to a plurality of second routers that act as multicast receivers;[0028,0067]

in response to the first request, the certificate authority creating and storing a

multicast session certificate that includes the encryption key, the multicast

session identifier, and the list of authorized multicast receivers;[0049,0050]

receiving, at the certificate authority from at least a particular second router of the

plurality of second routers, a second request to obtain the encryption key,

wherein the second request includes the multicast session identifier;[0047,0050]

in response to the second request,

determining whether the particular second router is included in the list of

authorized multicast receivers;

when the particular second router is included in the list of authorized multicast

receivers,

based on the multicast session identifier included in the second request

and the multicast session certificate, the certificate authority

retrieving the encryption key;[0028,0053,0062,0047] and

the certificate authority sending the encryption key to the particular

second router for use in decrypting the encrypted data[0029,0050].Trostle does not explicity teach Ipsec. However the use of IPsec is well known in the art. For example Turtiainen teaches use of IPsec in multicast system. Therefore it would be obvious to one having ordinary skill in the art at the invention was made to employ the method of

Turtianinen with the system of Trostle in order to achieve secure communication among multicast group communication.

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 571-272-3852. The examiner can normally be reached on 8-5.

38. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fikremariam Yalew

Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100